Álgebra Moderna II

R anillo conmutativo. le llamamos DOMINIO ENTERO si $a, b \in R$

$$a \cdot b = 0 \implies a = 0 \text{ ó } b = 0 \text{ en } R$$

EJEMPLO: $\mathbb{Z}$, $F[x]$ donde F es un dominio entero.
$\mathbb{Q}$, $\mathbb{C}$, $F \leftarrow$ campo.

NO EJEMPLO: $\mathbb{Z}/4\mathbb{Z}$ pues $2 \cdot 2 = 4 = 0$.

$$F = \left\{ a/b \;\middle|\; \begin{matrix} a \in R \\ b \neq 0 \end{matrix} \quad R \text{ dominio entero} \right\} \Big/ \sim \quad \leftarrow \text{CAMPO DE FRACCIONES}$$

$$\frac{a}{b} \sim \frac{a'}{b'} \iff ab' = a'b \text{ en } R$$

EJER: F es un campo.

OBSERVAR:

$$\begin{aligned} R &\hookrightarrow F \\ a &\longmapsto a/1 \end{aligned} \qquad \text{¡INCLUSIÓN!}$$

Por lo tanto, un dominio entero siempre está contenido en un campo.

EJEMPLOS: $\mathbb{Z} \hookrightarrow \mathbb{Q}$

$F[x] \hookrightarrow F(x)$

$\mathbb{Z}[i] \hookrightarrow \mathbb{Q}[i]$

Más estructura de los dominios enteros:

Factorización: en $\mathbb{Z}$.

0) Algoritmo de la división: $|a| < |b|$

$b = ma + r \quad 0 \leq r < |a|$.

Consecuencia:

1) Todo ideal $\neq 0$ de $\mathbb{Z}$ es principal, generado por el mínimo elemento de I.

(2) en particular $I=(a,b)=(d)$
con $d=ma+nb$, d es el
máximo común divisor de a & b.
(MCD existe)

(3) si p es primo & $p \mid ab$, entonces
$p \mid a$ o $p \mid b$.

<u>Demostración</u>: si $p \nmid a$ entonces
$$mcd(p,a)=1 \Rightarrow 1=am+np$$
$$\Rightarrow b=abm+npb \Rightarrow p \mid b.$$

(4) Cualquier entero tiene una factorización <u>única</u> en primos.
$$n=\pm p_1 p_2 \cdots p_k$$

Demostración: por inducción en el # de factores.

esbozo: $n = \pm p_1 \cdots p_l = q_1 \cdots q_l$; $l = k+1$

y suponemos el teorema es cierto cuando n tiene a lo más k factores.

de ③ $p_1 \mid q_2 \cdots q_l$ ó $p_1 = q_1$,

$\Rightarrow$ $p_1 = q_r$ para algún r.

$\Rightarrow$ $\frac{n}{p_1} = \frac{q_1 \cdots q_k}{p_1}$ tiene k factores y su descomposición en primos es única por hipótesis de inducción.

Por lo tanto Teorema fundamental de la aritmética se sigue del algoritmo de la división.

Otro ejemplo de un anillo con algoritmo de la división es $R = F[x]$, F campo

$$g(x) = f(x)\,q(x) + r(x) \quad \text{con} \quad \text{grado}(r(x)) < \text{grad}(f(x))$$

$\Rightarrow$ 1) Cualquier ideal es principal.

2) Cualesquiera f & g tienen un MCD.

$$(d) = (f, g) = I \leq R \text{ ideal}$$

$$d = m(x) f(x) + n(x) g(x)$$

(3) $p(x) \in R$ es ~~irreducible~~ primo si

cualquier factorización de $p = ab$

implica que grado$(a) = 0$ ó

grado$(b) = 0$.

$$\Rightarrow \quad (a,p) = \begin{cases} (1) \\ (p) \end{cases}$$

$\Rightarrow$ si $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.

(4) Cualquier $f \in R$ tiene una factorización única en primos,

$$f = u p_1 \cdots p_e \qquad u \in R^* = F^*$$

<u>Definición</u>: A un dominio, se le llama Euclidiano si $\exists$ una función

$$\delta : R \setminus \{0\} \longrightarrow \underbrace{\{1, 2, 3 \ldots\}}_{\mathbb{Z}_{\geq 1}}$$

tal que $\forall\ a, b \neq 0$ en R, tenemos

$b = ma + r$ con $r = 0$ ó

$$\delta(r) < \delta(a).$$

Eg: en $\mathbb{Z}$, $\delta(a) = |a|$

en $F[x]$; $\delta(f) = \deg(f) + 1$.

en $\mathbb{Z}[i]$, $\delta(\alpha) = a^2 + b^2$.

Algoritmo de la división en $\mathbb{Z}[i]$, (enteros gaussianos)

$A, B \in \mathbb{Z}[i]$ Intentemos dividir: B/A

$$= B\bar{A}/A\bar{A} = \frac{B\bar{A}}{\text{positive integ.}}$$

entonces

$B = Aw$ con $w = \alpha + \beta i$; $\alpha, \beta \in \mathbb{Q}$

$\alpha = \alpha_0 + r_0$ $\quad \alpha_0, \beta_0 \in \mathbb{Z}$ &

$\beta = \beta_0 + s_0$ $\quad -1/2 \leq r_0, s_0 < \frac{1}{2}$

entonces

$$B = A\underbrace{(\alpha_0 + \beta_0 i)}_{m} + \underbrace{A(r_0 + s_0 i)}_{R}$$

$$= Am + R$$

Afirmación: $$\delta(R) \leq \frac{1}{2}\delta(A)$$

Demostración:

$$\delta(R) = \delta(A)(r_0^2 + s_0^2)$$
$$\leq \delta(A)\left(\frac{1}{4}+\frac{1}{4}\right) = \frac{1}{2}\delta(A)$$

Este es el algoritmo de la división en $\mathbb{Z}[i]$.

Eg. $R = \{a+b\sqrt{-5} \mid a,b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{-5}]$

¿Euclidiano? $$\delta(a+b\sqrt{-5}) = a^2+5b^2$$

Esta función NO nos da un algoritmo de la división

De hecho: en R

(1) $$6 = 3 \cdot 2 = (1+\sqrt{-5})(1-\sqrt{-5})$$

donde todos los factores son primos.

(2) $I = (2, 1+\sqrt{-5})$ no es principal

$$R/I \cong \mathbb{Z}/2\mathbb{Z}$$

¿Es posible tener DIP sin que sea Dominio Euclidiano?

¿Es posible tener DFU sin que sea DIP?

$\mathbb{Z}, \mathbb{Z}[i]$ R Dominio Euclidiano

$\downarrow$

R DIP = Dominio de Ideales Principales.

$\downarrow$

R DFU = Dominio de Factorización Única.

↳ factorización en primos.

= Reformulemos divisibilidad, primo etc. en términos de ideales =

$a \mid b$ en $R \longrightarrow b = ma \quad m \in R$

$b \in (a) \iff$

$(b) \subseteq (a)$

P es primo (irreducible) si no es unidad & no tiene factores propios.

$(p) \subsetneq R$ maximal con respecto a ideales principales

$(p) \subseteq (\ ) \subseteq R$

principal

Si R es DIP, entonces $(p) \subseteq R$ maximal

$\Longleftrightarrow$ $R/(p)$ es campo.

$\Rightarrow$ $R/(p)$ es un dominio

— EJEMPLO: (De un dominio que no es DIP)

$R = \mathbb{Z}[x]$ $\quad I = (x)$ $\quad \underbrace{R/I \cong \mathbb{Z}}_{\text{no es un campo}}$

$\Rightarrow$ R no es DIP.

R
- No es Euclidiano
- No es DIP
- SI es DFU ⟵ !